Random selective block encryption technique for image cryptography using chaotic cryptography

Abstract: In this paper, we propose a dynamic random growth technique and hybrid chaotic map to perform block-based image encryption. Cat map can be easily cracked by the plaintext attack as it is periodic, and therefore cat map securely used in which it can eliminate the cyclical occurrence and withstand the effect of plaintext attack. The diffusion process calculates the intermediate parameters according to the image block. To generate the random data stream we use an intermediate parameter as the initial parameter in the chaotic map. In this manner, the generated data streams are dependent on the plain text image which can withstand the plain text attack. The results of this experiment prove that the proposed image encryption algorithm is secured one in which it can be used in image transmission systems.

Keywords: chaotic, encryption, decryption, permutation, diffusion

I. Introduction:

In the tremendous growth of multimedia and digital technology, the security of image has become a major issue for transmission and communication through the network. To sort out this issue, encryption is the right technique to protect the digital image/data. Image encryption is nothing but the transmission of data in an unreadable format in which it can be read-only by those members who have specific knowledge, commonly referred to as a key. Chaos concept has been proposed in the 1970s, which was used in mathematics, physics, engineering, biology, and so on. Chaos technique is used to transmit the information securely or privately through the third-party. The usage of chaos cryptography has become a much interesting one since it is being first investigated by Robert Matthews in 1989. To use the chaos theory effectively in cryptography, we must implement the chaotic maps in such a way that the entropy generated by the chaotic map can be able to construct required diffusion and confusion.

II. Related work:

1. May H. Abood [1]. Image Cryptography using Pixel Shuffling and Hash-LSB Steganography using RC4 stream cipher. Encrypt, Embedding and Decrypt are the three main process which is carried out to implement the image cryptography. The proposed system used the Shuffling algorithm and RC4 to encrypt the image. Hash-based Least Significant Bit(H-LSB) have been used to convert encrypted image to cover image. The encrypted 8-bit secret image is converted into a 4-bit of LSB of RGB pixels which is sent to the receiver. They conclude that hiding a

grayscale image inside the RGB image has more efficient value.

2. Shetty, A., Kiran, R., Shetty, S., Naik, S., Nayak, S., & D'Souza, D. J.[2]. The Introduction of prime numbers to encrypt an image is carried out. This prime number determines the number of shares which is sent to the receiver. PRNG is used for key generation in the encryption process. The encrypted image using the key is then used to generate a share which is then converted into the compressed file. This compressed file is sent to the receiver. On the other side, the compressed file is first decompressed and then decrypted using the key. The proposed technique overcomes side-channel attacks and algebraic attacks.

3. Kaur, A., & Singh, G. [3]. Image encryption and decryption with Random Selective Block encryption technique using Blowfish Algorithm. The random selective block technique first divides the image into an equal number of blocks. Then it selects the block randomly and increases the pixel level for the encryption process. Both encrypted block and non-encrypted block join together to provide a complete encrypted image.

4. Wang, Xingyuan, Siwei Wang, Yingqian Zhang, and Kang Guo.[4]. Based on multiple one-dimensional logistic chaotic shuffling methods, a novel encryption scheme has been proposed. It has two main phases. One is shuffling and another one is diffusion. In the shuffling stage, the coordinates are determined by the two logistic maps. A new design has been proposed for a quick exchange of pixel locations. In the diffusion stage, MOD operation and XOR operation is used to diffuse the image. The proposed system shows that this image encryption scheme has a high-security level.

5. Alzubaidi, A. M. N. [5]. An encryption scheme has been proposed on the bases of a 3D logistic transform. The RGB image is converted into three different channels that are Y, Cb and Cr images. Selective encryption and chaotic encryption method have been applied to Y components. 2D Arnold Cat is used to adopt the confusion method. 2D Baker map is applied to Cb and Cr in a row-wise and column-wise approach. Now, all the encrypted Y, Cb, and Cr are combined to provide a Cipher image.

6. Pak, C., & Huang, L.[6]. Image encryption using the combination of 1D chaotic map. Chaotic model is evaluated using three different mapping techniques they are Logistic, Sine and Chebyshev. A new chaotic map is created using the three mapping techniques and its accuracy has been demonstrated. The encryption algorithm of the linear and non-linear structures has been performed. The original image has a different histogram level but after encryption, all the encrypted has been performed with the same histogram level.

7. Liu, W., Sun, K., & Zhu, C. [7]. Based on the chaotic mapping, a fast image encryption algorithm is performed. The model of 2D-SIMM

has been established to enlarge the keyspace. CST based encryption has been introduced to obtain a better scrambling effect and also the time-complexity and security have been analyzed. To improve the security of the image, a combination-decomposition mechanism has been presented to encrypt the color image.

8. Li, Y., Wang, C., & Chen, H.[8]. Using pixel-level permutation and bit-level permutation an hyper-chaos-based image encryption algorithm has been introduced. This algorithm supports 5D multi-wing hyperchaotic system. Both the permutation process employed to strengthen the security of the cryptosystem. To change the pixel diffusion operation has been performed. The hyper-chaotic system is carried out to resist the general method which can decipher the low-dimension chaotic map. The bit-level permutation is done to scramble the image. Compared to other hyper-chaos this algorithm is safer because of the combination of bit-level permutation and pixel-level permutation with the hyper-chaos algorithm.

9. Fouda, J. A. E., Effa, J. Y., Sabat, S. L., & Ali, M.[9]. Image encryption by fast chaotic cipher technique has been studied. The encryption process is carried out by generating a chaotic number, LDE solutions, permutation, and diffusion keys. Keyspace analysis and statistical analysis is performed. A combination of a chaotic system and LDE helps to generate large permutation and diffusion keys faster. Instead of generating the permutation for each sub-image, the proposed algorithm dynamically updates four integers in the permutation with the help of the chaotic system.

10. Abanda, Y., & Tiedeu, A. [10]. Image encryption by chaos mixing. Much chaos technique has been implemented in the image encryption process. In this study, they suggest an approach using two oscillators they are Colpitts and duffing which helps to increase the keyspace. Histogram mapping for both original and encrypted images is performed. As a result, the efficiency of the algorithm is demonstrated.

III. Proposed system:

Chaotic Cryptography:

Chaotic Cryptography is a mathematical application based on Chaos theory. It is used to transmit the data in a secured manner. To use chaos theory, chaotic maps are implemented so that the entropy is generated with the help of a chaotic map which can produce the required confusion and diffusion.

Entropy:

It relates the amount of uncertainty about an event or a process associated with the given probability distribution.

$$S = -\sum_i P_i \log P_i = -\operatorname{E}_P[\log P]$$

Where,

P – Probability of occurance

Logistic regression:

Logistic regression classifies the data on extreme ends by considering the outcome variables.

Permutation process:

For M x M image, we use logistic maps in this process

$$f : X_{n+1} = \mu X_n(1-X_n)$$

Where,

Xn - independent variable

μ- control parameter of logistic maps

n - 0, 1, 2…

Diffusion process:

We used another logistic mapping in the diffusion process.

$$h : x'_{n+1} = \mu' x'(1-x'_n)$$

Encryption steps:

TABLE 1 Encryption Description

Step	Process	Description
1	Select the image	The image can be any ratio. It can even be in any format. Both grayscale and colour image are accepted
2	Colour image into grayscale	When we select a colour image then this step is required. We have to convert the colour image into a grayscale image. For this conversion we required a predefined function-rgb2gray(img). This function converts the colour image to a grayscale image.
3	Blockwise split	The converted grayscale image is then split into n number of blocks. These blocks are jumbled by changing its position. The new position of the block can be found by applying row and column shift.
4	Key	The key is generated using the Diffusion matrix. To get the key we need to do XOR function on k and ktemp. This key is used to do encrypt and decrypt for the selected image.
5	Encryption	Encryption is generated using the key and block-wise split image. Encryption is the process to hide the selected image and send that to the receiver. The receiver cannot view the image until they know the key and encrypted image. By knowing the key and encrypted image we can able to get the original image.

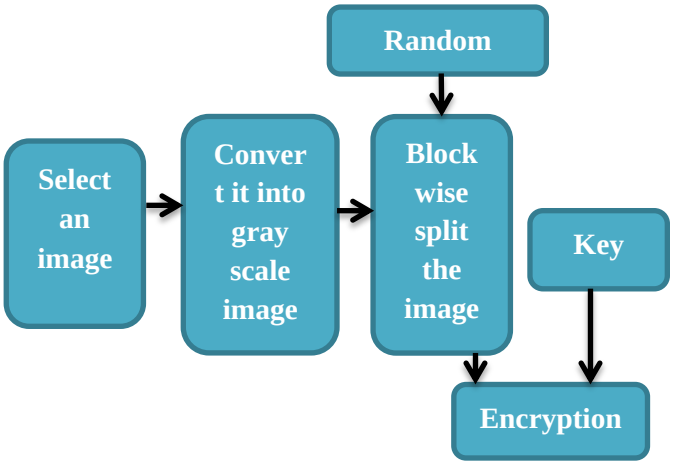

Fig. 1 Encryption steps

TABLE 2 Decryption Description

Step	Process	Description
1	Encrypted image	This encrypted image is generated from the encryption process. The encrypted image has invisible detail in it. This can be viewed only when we have the key.
2	Key	The key is obtained in the encryption process.
3	Decryption	Decryption is generated using by applying XOR to encrypted image and key generated.

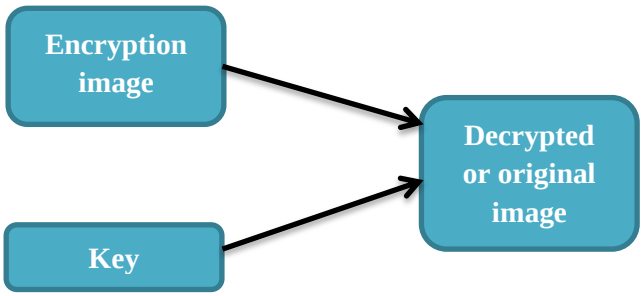

Fig. 2 Decryption steps

IV. Result and discussion process:

This project can be run using Matlab. It does not require any additional tool or library to run this project. Then follow the step to get the output as explained above.

Select an image either in grayscale or RGB format as mentioned above. If we have a select RGB image then we need to convert it into grayscale using a predefined function **rgb2gray(img).**

Fig 2 is the original image that has been selected for the process. This image has already converted into grayscale so that we won't use the rgb2gray(img) function.

Fig. 3 Original image

In figure 3 we get the encrypted image. The encrypted image is obtained by following the steps that are discussed above. This encrypted image is split into the block which is encrypted.

The encryption is done using the key and plain image. The temple image is encrypted here in which we can able to read the image properly without using key and decryption steps.

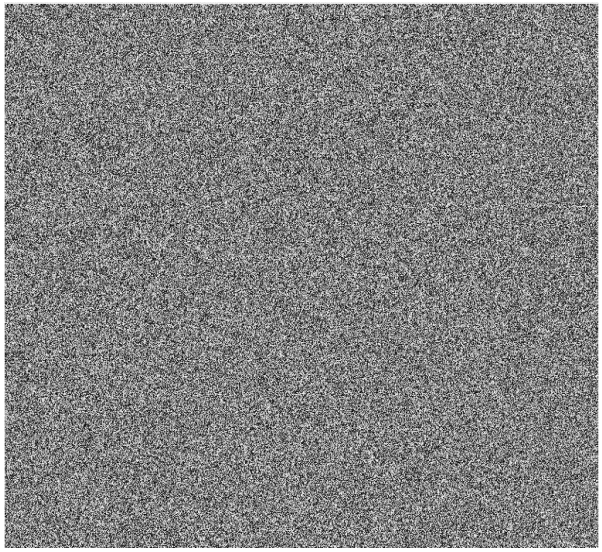

Fig. 4 Encrypted image

Figure 4 is about decryption. The reverse process of encryption is decryption. By using the key and encrypted image we can able to get the decrypted image. The encrypted temple image and key generated are used to get the decrypted or original temple image.

Fig. 5 Decrypted image

Figure 5 is about the histogram of the original image. The histogram is obtained for the original temple image. For the original temple image, the histogram is unevenly spread.

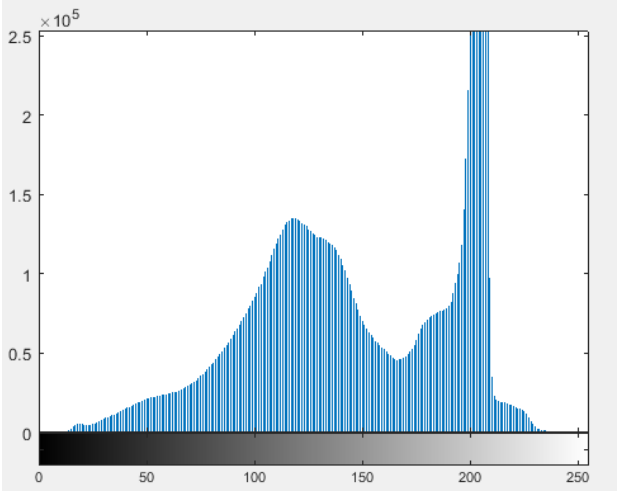

Fig. 6 Histogram of the original image

Figure 6 is about the histogram of the encrypted image. The temple is first encrypted and the histogram is found out for the encrypted image. The histogram of the encrypted image is evenly separated and the frequency value does not change often.

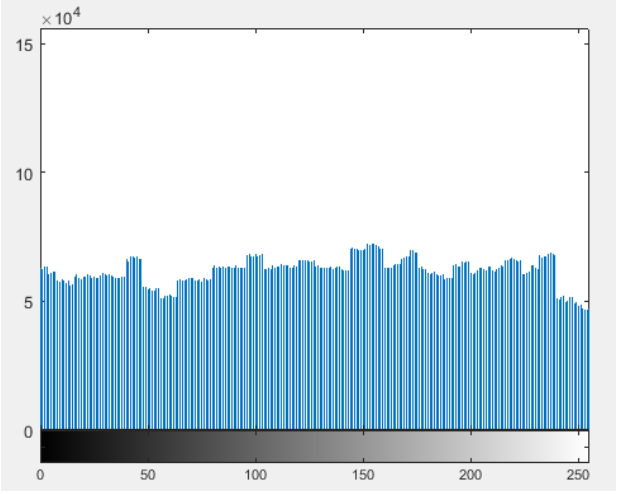

Fig. 7 Histogram of the encrypted image

In figure 7 pixel correlation is shown. In the pixel correlation graph, there are two divisions. One is the pixel correlation of the original image and the other is the pixel correlation of encrypted image. Each pixel correlation side has three graphs- 1) horizontally, 2) vertically, 3) dimensionally. For the original temple image, the pixel correlation almost lies in the same place. So it may be secure whereas in the encrypted image the pixel correlation is scattered in all values. Hence the encrypted image is secure.

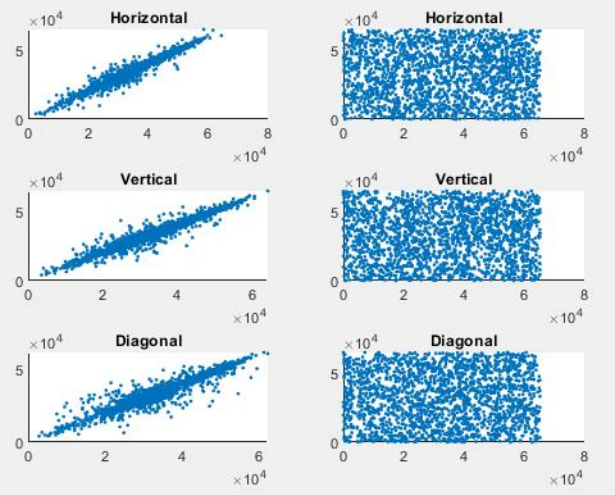

Fig. 8 Pixel correlation

V. Conclusion:

This paper discusses, how hybrid chaotic map and dynamic random growth technique is efficiently used to encrypt the digital image and to decrypt the image. The applications of a chaotic system in an image processing technique are image encryption and image compression. By using an improved cat map we have performed fast image encryption. The main usage of dynamic random growth technique is to enhance the security of the data being transmitted. The pixel diffusion process totally depends upon the plain text and key. The proposed scheme can withstand any chosen plain text attacks and it performs secured transmission of the data.

Reference:

[1] Abood, M. H. (2017, March). An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. In 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT) (pp. 86-90). IEEE.

[2] Shetty, A., Kiran, R., Shetty, S., Naik, S., Nayak, S., & D'Souza, D. J. (2017, September). Image cryptography using RNS algorithm. In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) (pp. 1936-1939). IEEE.

[3] Kaur, A., & Singh, G. (2018, April). A Random Selective Block Encryption Technique for Secure Image Cryptography Using Blowfish Algorithm. In 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 1290-1293). IEEE.

[4] Wang, Xingyuan, Siwei Wang, Yingqian Zhang, and Kang Guo. "A novel image encryption

algorithm based on chaotic shuffling method." Information Security Journal: A Global Perspective 26, no. 1 (2017): 7-16.

[5] Alzubaidi, A. M. N. (2014). Selective Image Encryption with Diffusion and Confusion Mechanism. International Journal, 4(7).

[6] Pak, C., & Huang, L. (2017). A new color image encryption using combination of the 1D chaotic map. Signal Processing, 138, 129-137.

[7] Liu, W., Sun, K., & Zhu, C. (2016). A fast image encryption algorithm based on chaotic map. Optics and Lasers in Engineering, 84, 26-36.

2-750.

[8] Li, Y., Wang, C., & Chen, H. (2017). A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Optics and Lasers in Engineering, 90, 238-246.

[9] Fouda, J. A. E., Effa, J. Y., Sabat, S. L., & Ali, M. (2014). A fast chaotic block cipher for image encryption. Communications in Nonlinear Science and Numerical Simulation, 19(3), 578-588.

[10] Abanda, Y., & Tiedeu, A. (2016). Image encryption by chaos mixing. IET Image Processing, 10(10), 74